

70. (New) The method as recited in claim 69, further comprising submitting the signed software identity register over a network to a third party to prove an identity of the operating system to the third party.

71. (New) The method as recited in claim 69, wherein creating an identity of the OS comprises forming the OS certificate with one or more items from a boot log containing identities of software components that are executing on the CPU.

72. (New) The method as recited in claim 69, wherein the identity of the OS further contains the CPU public key.

73. (New) For execution on a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a pair of private and public keys and a software identity register that holds an identity of the operating system, a computer program stored on one or more computer-readable storage media of the computer system, the program comprising:

forming an OS certificate containing the identity from the software identity register and information describing the operating system; and

signing the software identity register using the CPU private key.

74. (New) The computer program stored on one or more computer-readable storage media as recited in claim 73, further comprising submitting the

signed software identity register over a network to a third party to prove an identity of the operating system to the third party.

75. (New) The computer program stored on one or more computer-readable storage media as recited in claim 73, wherein the OS certificate further contains the CPU public key.

76. (New) In a computer system having a central processing unit and an operating system, the central processing unit having a pair of private and public keys and a software identity register that holds an identity of the operating system, a method comprising signing the software identity register using the private key of the pair of private and public keys.

77. (New) The method as recited in claim 76, further comprising submitting the signed software identity register over a network to a third party to prove an identity of the operating system to the third party.

---